Logarithmic-size Non-Interactive Zero-Knowledge Proofs for Arithmetic Circuits

Advisor(s): Sebastian Ramacher

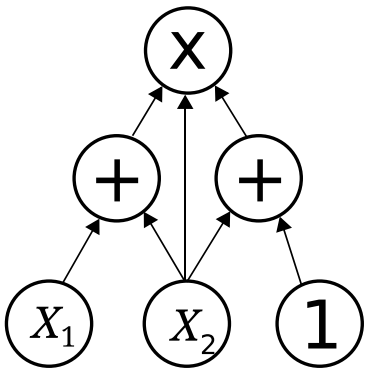
Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Austria

Motivation

Non-interactive zero-knowledge (NIZK) proofs allow a prover to convince a verifier that it possess knowledge of some secret value without actually revealing said information. Such NIZK proofs can be used to build digital signature schemes from one-way functions. Picnic, a post-quantum signature scheme, uses NIZK proof for general circuits name ZKB++ and instantiates the one-way function from a block cipher. In that case the size of the proof – and thus signatures – is linear in the size of the underlying circuit.
Recent improvements such as Ligero improve the size of the proofs to be logarithmic in the size of the circuit. However, these improvements come at a cost: Ligero has to account for XOR and AND gates in the proof size, but the size of ZKB++ proofs only depend on the number of AND gates. Thus the choice block ciphers used to instantiate the one-way function depends on the NIZK proof system.
Your task is to implement Ligero and then evaluate circuits of block ciphers with respect to their performance in terms of proof size and runtime performance.

Goals and Tasks

- Get familiar with Ligero.
- Implement Ligero and experiment with different circuits (LowMC, MiMC).
- Compare proof sizes to ZKB++ based NIZK proofs.



Arithmetic circuit (Tcshasaposse, CC-BY-SA 3.0).

Literature

- S. Ames et al.
  Ligero: Lightweight Sublinear Arguments Without a Trusted Setup
  CCS
- M. Chase et al.
  Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives
  CCS

Deliverables

- Project files (zip, cleaned)
- Documentation (pdf)
- Presentation (pdf)

Schedule

- Start Immediately
- Month 1 Reading literature
- Month 2 Implementing
- Month 3 Final deliverables

Studies

☒ INF ☒ TEL ☒ SW

Prerequisites

- Basic cryptographic background
- Programming

Advisor / Contact

sebastian.ramacher@iaik.tugraz.at